AMENDMENTS TO THE CLAIMS

For the convenience of the Examiner, all claims have been presented whether or not an amendment has been made. The claims have been amended as follows:

1. (Currently Amended) Apparatus for multiplication of modular numbers, comprising:

a two-dimensional dependency array of selectively coupled cells, where each cell comprises:

a first full adder receiving a first input signal, a second input signal, and a clock ~~signal,~~ signal; and

a second full adder receiving an output of the first full adder, a third input signal, and a clock signal;

the coupled cells being operable to perform an input-to-output transfer relationship wherein:

a product output comprises a remainder of a variable modulus two, the product output representing a first number multiplied by a second number;

the variable comprises a sum of a product input, a first product, a second product, and a quotient input, the first product representing an integer value multiplied by a modulus value, the second product related to a product of the first number and the second number;

a quotient output comprises the variable divided by two; and

the integer value comprises a remainder of the product input modulus two;

a half adder receiving an output of the second full adder and a fourth input signal;

a first storage circuit coupled to the second full adder;

a second storage circuit coupled to the half adder; and

a third storage circuit coupled to the half adder.

2. (Previously Presented) Apparatus for multiplication of modular numbers as in Claim 1 wherein the two-dimensional dependency array comprises a row by column configuration of selectively coupled cells.

3. (Original) Apparatus for multiplication of modular numbers as in Claim 1 wherein the two-dimensional dependency array comprises groups of two dependency graph cells coupled together to add within one pair of cells product terms of equal weight.

4. (Original) Apparatus for multiplication of modular numbers as in Claim 1 further comprising a binary number reduction circuit sequentially coupled to the output of the two-dimensional dependency array of cells.

5. (Currently Amended) Apparatus for multiplication of modular numbers, comprising:

a two-dimensional dependency array of selectively coupled cells, wherein each cell comprises:

a first full adder receiving a first input signal, a second input signal, and a clock signal;

a second full adder receiving a third input signal, a fourth input signal, and a clock signal;

a third full adder receiving an output of the second full adder, a fifth input signal, and an output of the first full adder, and providing an output signal;

a fourth full adder receiving an input from the first full adder, an input from the second full adder and providing an output to the first full adder;

a first storage circuit coupled between the second full adder and the third full adder;

a second storage circuit coupled between the fourth full adder and the first full adder; and

a third storage circuit in a feedback loop coupled to the fourth full adder, the fourth adder receiving an input from the third storage circuit;

the coupled cells being operable to perform an input-to-output transfer relationship wherein:

a product output comprises a remainder of a variable modulus two, the product output representing a first number multiplied by a second number;

the variable comprises a sum of a product input, a first product, a second product, and a quotient input, the first product representing an integer value multiplied by a modulus value, the second product related to a product of the first number and the second number;

a quotient output comprises the variable divided by two; and

the integer value comprises a remainder of the product input modulus two.

6. (Original) Apparatus for multiplication of modular numbers as in Claim 5 further comprising a reduction circuit coupled to the two-dimensional dependency array and sequentially receiving signals therefrom.

7. (Previously Presented) Apparatus for multiplication of modular numbers as in Claim 6 wherein said reduction circuit comprises a row by column array of selectively coupled cells.

8. (Previously Presented) Apparatus for multiplication of modular numbers as in Claim 6 wherein the two-dimensional dependency array of selectively coupled cells comprises a binary multiplier, and the reduction circuit comprises concurrent reduction sequentially receiving signals from the binary multiplier.

9. (Currently Amended) Apparatus for multiplication of modular numbers, comprising:

a serial array of interconnected cells each comprising:

a first full adder receiving a first input signal, a second input signal, and a clock signal;

a first storage circuit coupled in a feedback loop between an output of the first full adder and an input thereto;

a second storage circuit receiving the first input signal and providing an output signal; and

a third storage circuit coupled to the first full adder and the second storage circuit and providing an output to the adjacent ~~cell~~ cell; and

a concurrent reduction cell comprising:

a first full adder receiving a first input signal, a second input signal, and a clock signal;

a second full adder receiving an output of the first full adder, a third input signal, and a clock signal;

a first storage circuit coupled to an output of the first full adder and an input thereto;

a second storage circuit coupled to an output of the second full adder and an input thereto;

a third storage circuit coupled to an output of the first full adder and providing an output; and

a fourth storage circuit coupled to the second storage circuit and the second full adder.

10. (Original) Apparatus for multiplication of modular numbers as in Claim 9 wherein adjacent cells are interconnected in a serial adder configuration.

11. (Cancelled)

12. (Previously Presented) Apparatus for multiplication of modular numbers as in Claim 9 further comprising:

a first serial shift register having as an output a signal coupled to the first cell in the serial configuration;

a second serial shift register providing the second input to the first full adder of the first cell in the serial configuration; and

a third serial shift register serially receiving an output from the third storage circuit of the last serial adder in the serial configuration and providing a parallel output signal.

13. (Currently Amended) Apparatus for multiplication of modular numbers, comprising:

a plurality of locally related cells coupled in a two-dimensional dependency array, each of the plurality of locally related cells comprising a computing circuit; and

an input-to-output transfer relationship for the coupled cells ~~given by:~~ wherein:

~~$X_{out} = (X_{in} + x_j * n_i + a_i * b_j + t_{in})$ mod 2,~~

~~$e_{out} = (X_{in} + x_j * n_i + a_i * b_j + t_{in})$ div 2,~~

~~$x_j = X_{in}$ mod 2,~~

~~$a_{out} = a_{in}$;~~

~~$b_{out} = b_{in}$~~

~~$n_{out} = n_{in}$~~

a product output comprises a remainder of a variable modulus two, the product output representing a first number multiplied by a second number;

the variable comprises a sum of a product input, a first product, a second product, and a quotient input, the first product representing an integer value multiplied by a modulus value, the second product related to a product of the first number and the second number;

a quotient output comprises the variable divided by two; and

the integer value comprises a remainder of the product input modulus two.

14. (Previously Presented) Apparatus for multiplication of modular numbers as in Claim 13 further comprising a signal flow graph connecting to the cells coupled in the two-dimensional dependency array.

15. (Previously Presented) Apparatus for multiplication of modular numbers as in Claim 13 wherein the two-dimensional dependency array comprises a row-by-column configuration of selectively coupled cells.

16. (Previously Presented) Apparatus for multiplication of modular numbers as in Claim 13 wherein the two-dimensional dependency array comprises groups of two dependency graph cells coupled together to add within one pair of cells product terms of equal weight.

17. (Previously Presented) Apparatus for multiplication of modular numbers as in Claim 13 wherein the two-dimensional dependency array comprises a linear array of computational cells comprising:

a first full adder receiving a first input signal, a second input signal, and a clock signal,

a second full adder receiving an output of the first full adder, a third input signal, and a clock signal;

a half adder receiving an output of the second full adder and a fourth input signal;

a first storage circuit coupled to the second full adder;

a second storage circuit coupled to the half adder; and

a third storage circuit coupled to the half adder.

18. (Currently Amended) Apparatus for multiplication of modular numbers, comprising:

a multiplication stage comprising a plurality of locally related cells coupled in a two-dimensional dependency array;

a reduction stage comprising a plurality of locally related cells coupled in a two-dimensional dependency array, wherein the reduction stage couples to the multiplication stage; and

an input-to-output transfer relationship for the coupled cells in the multiplication stage and the reduction stage ~~given by:~~ wherein:

~~$X_{out} = (X_{in} + x_j * n_k + e_{in})$ mod 2,~~

~~$e_{out} = (X_{in} + x_j * n_k + e_{in})$ div 2,~~

~~$x_j = X_{in}$ mod 2,~~

~~$n_{out} = n_{in}$~~

a product output comprises a remainder of a variable modulus two, the product output representing a first number multiplied by a second number;

the variable comprises a sum of a product input, a first product, and a quotient input, the first product representing an integer value multiplied by a modulus value;

a quotient output comprises the variable divided by two; and

the integer value comprises a remainder of the product input modulus two.

19. (Previously Presented) Apparatus for multiplication of modular numbers as in Claim 18 wherein the multiplication stage two-dimensional dependency array and the reduction stage two-dimensional dependency array comprises a linear array of interconnected cells each comprising:

a first full adder receiving a first input signal, a second input signal, and a clock signal;

a first storage circuit coupled in a feedback loop between an output of the first full adder and an input thereto;

a second storage circuit receiving the first input signal and providing an output signal;

a third storage circuit coupled to the first full adder and the second storage circuit and providing an output to the adjacent cell.

20. (Previously Presented) Apparatus for multiplication of modular numbers as in Claim 19 wherein the reduction stage two-dimensional dependency array comprises an array of computational cells comprising:

a first full adder receiving a first input signal, a second input signal, and a clock signal;

a second full adder receiving an output of the first full adder, a third input signal, and a clock signal;

a first storage circuit coupled to an output of the first full adder and an input thereto;

a second storage circuit coupled to an output of the second full adder and an input thereto;

a third storage circuit coupled to an output of the first full adder and providing an output; and

a fourth storage circuit coupled to the second storage circuit and the second full adder.

21. (Previously Presented) Apparatus for multiplication of modular numbers as in Claim 18 wherein the multiplication stage two-dimensional dependency array and the reduction stage two-dimensional dependency array each comprises a row-by-column configuration of selectively coupled cells.

22. (Currently Amended) A method for multiplication of modular numbers comprising:

coupling a plurality of locally related cells in a two-dimensional dependency array, each of the plurality of locally related cells comprising a computing circuit; and

providing an input-to-output transfer relationship for the coupled cells ~~as given by:~~ wherein:

~~$X_{out} = (X_{in} + x_j * n_i + a_i * b_j + t_{in})$ mod 2,~~

~~$e_{out} = (X_{in} + x_j * n_i + a_i * b_j + t_{in})$ div 2,~~

~~$x_j = X_{in}$ mod 2,~~

~~$a_{out} = a_{in}$;~~

~~$b_{out} = b_{in}$~~

~~$n_{out} = n_{in}$~~

a product output comprises a remainder of a variable modulus two, the product output representing a first number multiplied by a second number;

the variable comprises a sum of a product input, a first product, a second product, and a quotient input, the first product representing an integer value multiplied by a modulus value, the second product related to a product of the first number and the second number;

a quotient output comprises the variable divided by two; and

the integer value comprises a remainder of the product input modulus two.

23. (Previously Presented) The method for multiplication of modular numbers as in Claim 22 further comprising mapping the cells of the two-dimensional dependency array onto a signal flow graph comprising a linear array of cells.

24. (Previously Presented) The method for multiplication of modular numbers as in Claim 22 wherein coupling the plurality of locally related cells comprises coupling the cells to a near neighbor cell.

25. (Currently Amended) A method for multiplication of modular numbers, comprising:

coupling a first plurality of locally related cells as a multiplication stage in a two-dimensional dependency array, each of the plurality of locally related cells comprising a computing circuit;

coupling a second plurality of locally related cells as a reduction stage in a two-dimensional dependency array; and

providing an input-to-output transfer relationship for the coupled cells of the multiplication stage and the coupled cells of the reduction stage ~~as given by:~~ wherein:

~~$X_{out} = (X_{in} + x_j * n_k + e_{in})$ mod 2,~~

~~$e_{out} = (X_{in} + x_j * n_k + e_{in})$ div 2,~~

~~$x_j = X_{in}$ mod 2,~~

~~$n_{out} = n_{in}$~~

a product output comprises a remainder of a variable modulus two, the product output representing a first number multiplied by a second number;

the variable comprises a sum of a product input, a first product, and a quotient input, the first product representing an integer value multiplied by a modulus value;

a quotient output comprises the variable divided by two; and

the integer value comprises a remainder of the product input modulus two.

26. (Previously Presented) A method for multiplication of modular numbers as in Claim 25 wherein coupling the first plurality of locally related cells and the second plurality of locally related cells comprises coupling the cells of each plurality in a row-by-column configuration of selectively coupled cells.

27. (Previously Presented) The method for multiplication of modular numbers as in Claim 26 wherein coupling the first plurality of locally related cells and the second plurality of locally related cells comprises coupling cells together to add within one pair of cells product terms of equal weight.